IN THE CLAIMS

Claims 1-16 are cancelled.

17. (New) Validity verification method for a network key in a digital domestic network comprising at least a broadcasting device and a processing device, the broadcasting device having encrypted data to broadcast to the processing device, these data being accessible by the processing device thanks to a network key unknown by the broadcasting device, this method comprising following steps:

- transmission of a test key by the broadcasting device to the processing device,

- calculation of a cryptogram in the processing device resulting from the test key encryption by the network key,

- sending of the cryptogram to the broadcasting device,

- determination of the network key validity by the broadcasting device by comparing the cryptogram with a list of control cryptograms.

18. (New) Verification method according to claim 17, wherein the test key and the list of control cryptograms constitute control data and are generated in a verification center and transferred in the broadcasting device.

19. (New) Verification method according to claim 17, wherein the test key is determined by the broadcasting device, the list of control cryptograms is calculated by the broadcasting device on the base of a predetermined list of network keys transmitted by a verification center and constituting the control data, each control cryptogram being the result of the encryption of a listed network key with the test key.

20. (New) Verification method according to claim 19, wherein the test key is randomly generated and serves also as session key for the encryption of the encrypted data.

21. (New) Verification method according to claim 19, wherein the broadcasting device generates at least two test keys and transmit them to the processing device, which sends back to it the corresponding cryptograms and its associated test key for the verification operations and an other cryptogram and its associated test key as session key for the data encryption.

22. (New) Verification method according to claim 18, wherein the list of control cryptograms consists of a black list containing the cryptograms obtained by the encryption of the test key with invalid network keys.

23. (New) Verification method according to claim 18, wherein the list of control cryptograms consists of a white list containing the cryptograms obtained by the encryption of the test key with valid network keys.

24. (New) Verification method according to claim 22, wherein a cryptogram present in the black list or absent from the white list is refused during the comparison, an error signalization inviting the user to change the terminal module is then generated.

25. (New) Verification method according to claim 17, wherein the broadcasting device comprises a converter module in charge of the verification operations.

26. (New) Verification method according to claim 17, wherein the processing device comprises a terminal module storing the network key.

27. (New) Verification method according to claim 25, wherein the control list is stored in a memory of the broadcasting device, the comparison with the cryptogram is carried out by this device.

28. (New) Verification method according to claim 19, wherein the control data consist of an address indicating where the control list can be downloaded via Internet by means of the broadcasting device, said list is then stored in the memory of the broadcasting device.

29. (New) Verification method according to claim 25, wherein the converter module verifies the authenticity of the control list by means of a signature on said data.

30. (New) Verification method according to claim 17 wherein the control list is stored by a verification center, the broadcasting device transmits the cryptogram to said center for carrying out the verification.

31. (New) Verification method according to claim 19, wherein the broadcasting device is a DVD disc reader, this disc comprising on one hand the encrypted data and on the other hand the control data.

32. (New) Verification method according to claim 19, wherein the broadcasting device is a pay television decoder receiving the encrypted data and the control data from a managing center.

33. (New) Verification method according to claim 23, wherein a cryptogram present in the black list or absent from the white list is refused during the comparison, an error signalization inviting the user to change the terminal module is then generated.